REMARKS

Claims 1, 24 and 47 have been amended to further clarify the present invention. Support for claim amendments can be found at page 11, lines 13-14 of the specification. Claims 1, 4-6, 8-24, 27-29 and 31-47 are currently pending and under consideration. Reconsideration is respectfully requested.

I.   REJECTION OF CLAIMS 1, 4-6, 8-24, 27-29 AND 31-47 UNDER 35 U.S.C. 102(b) AS BEING ANTICIPATED BY HUFF ET AL. (WO 99/57625)(previously cited):

Claim 1 has been amended to recite a system for managing information comprising "a reflection unit which reflects the information collected and regulated by the information collection unit upon the database, to thereby predict a possible attack event or a leakage event in advance, and to avoid the predicted attack event or leakage event before execution of the predicted attack event or leakage event, wherein the information notified by the communication request monitor unit and/or countermeasure selected by the management unit are weighted".

At page 3 of the Office Action, the Examiner asserts that "a predicted attack" could be a later stage of an already executing attack. Therefore, independent claims 1, 24 and 47 have been amended to clarify "a predicted attack" according to the present invention.

Again, Huff et al. fails to disclose all of the features recited in claim 1, for example. That is, Huff et al. fails to disclose "to thereby predict a possible attack event or a leakage event in advance, and to avoid the predicted attack event or leakage event before execution of the predicted attack event or leakage event," as recited in amended claim 1, for example.

Instead, Huff et al. discloses a method and apparatus for receiving information that an intrusion or misuse has occurred and taking countermeasures on a computer network (see page 4, lines 17-20). The security computer system can automatically take countermeasures against the suspected or actual intrusion or misuse. Automatic countermeasures include using a defensive countermeasure to increase an auditing level conducted by an intrusion detection mission. An offensive countermeasure is also used to send a chase mission to the suspected or actual intruder. The offensive chase mission can be automatically dispatched with human intervention. Further, as pointed out by the Examiner, in Huff et al., an offensive agent is deployed to instruct a service request processor to dispatch a chase mission to a node from which the suspected intrusion is taking place. The chase mission then sends information to a service manager regarding the suspected intruder including an address and other information contained on the suspected intruder's computer (see column 21, lines 6-13). That is, in Huff et

al., a countermeasure is only carried out <u>after</u> the detection of an actual intrusion or suspected misuse. Thus, in <u>Huff et al.</u>, defensive steps are taken to halt further intrusion or misuse (see page 4, lines 15-16).

Although the above comments are specifically directed to claim 1, it is respectfully submitted that the comments would be helpful in understanding differences of various other rejected claims over the cited reference. Therefore, it is respectfully submitted that the rejection is overcome.
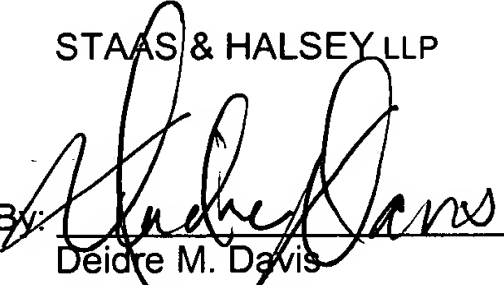
II.   CONCLUSION:

In view of the foregoing amendments and remarks, it is respectfully submitted that each of the claims patentably distinguishes over the prior art, and therefore, defines allowable subject matter. A prompt and favorable reconsideration of the rejection along with an indication of allowability of all pending claims are therefore respectfully requested.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: <u>June 2, 2006</u>

By: _____
Deidre M. Davis
Registration No. 52,797

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501